

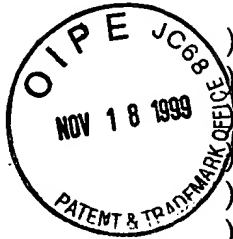
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Fumihiko SANO et al

Serial No.: 09/388,388

Filed: September 1, 1999



Group Art Unit: 2766

Examiner: Not Assigned

For: ENCRYPTION/DECRYPTION UNIT AND STORAGE MEDIUM

CLAIM FOR PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

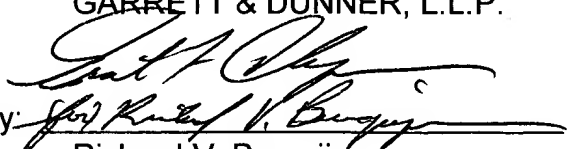
Under the provisions of 35 U.S.C. § 119, Applicants hereby claim the benefit of the filing date of Japanese Patent Application No. 10-337108, filed on November 27, 1998, for the above-identified U.S. patent application.

In support of Applicants' claim for priority, filed herewith a certified copy of the above.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

By:


Richard V. Burgujian
Reg. No. 31,744

Dated: November 18, 1999
RVB/FPD/sci
Enclosure

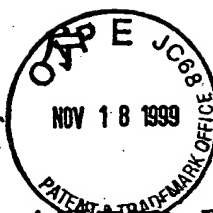
ERNEST F. CHAPMAN
Reg. No. 25,961

BEST AVAILABLE COPY

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N.W.
WASHINGTON, D.C. 20005
202-408-4000

日 本 国 特 許
PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
at this Office.

出 願 年 月 日
Date of Application:

1998年11月27日

出 願 番 号
Application Number:

平成10年特許願第337108号

出 願 人
Applicant(s):

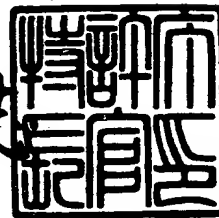
株式会社東芝

CERTIFIED COPY OF
PRIORITY DOCUMENT

1999年 8月16日

特許庁長官
Commissioner,
Patent Office

伴佐山 建志



【書類名】 特許願

【整理番号】 A009807445

【提出日】 平成10年11月27日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 7/00

【発明の名称】 暗復号装置及び記憶媒体

【請求項の数】 9

【発明者】

 【住所又は居所】 東京都府中市東芝町1番地 株式会社東芝府中工場内

 【氏名】 佐野 文彦

【発明者】

 【住所又は居所】 東京都府中市東芝町1番地 株式会社東芝府中工場内

 【氏名】 川村 信一

【発明者】

 【住所又は居所】 東京都府中市東芝町1番地 株式会社東芝府中工場内

 【氏名】 清水 秀夫

【特許出願人】

 【識別番号】 000003078

 【氏名又は名称】 株式会社 東芝

【代理人】

 【識別番号】 100058479

 【弁理士】

 【氏名又は名称】 鈴江 武彦

 【電話番号】 03-3502-3181

【選任した代理人】

 【識別番号】 100084618

 【弁理士】

 【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗復号装置及び記憶媒体

【特許請求の範囲】

【請求項 1】 平文を暗号文に暗号化し、及び又は、暗号文を平文に復号する暗復号装置であって、

暗号処理又は復号処理を行う第 1 の暗復号化手段と、

前記第 1 の暗復号化手段の出力を所定の置換表によりデータ置換する第 1 の置換手段と、

前記第 1 の置換手段の出力に対し、暗号処理又は復号処理を行う第 2 の暗復号化手段と、

前記第 2 の暗復号化手段の出力を所定の置換表によりデータ置換する第 2 の置換手段と、

前記第 2 の置換手段の出力に対し、暗号処理又は復号処理を行う第 3 の暗復号化手段と

を備えたことを特徴とする暗復号装置。

【請求項 2】 前記第 1 の暗復号化手段と前記第 3 の暗復号化手段、並びに、前記第 1 の置換手段と前記第 2 の置換手段は、それぞれ同一のアルゴリズムに従う手段となることを特徴とする請求項 1 記載の暗復号装置。

【請求項 3】 前記第 1、第 2 及び第 3 の暗復号化手段並びに前記第 1 及び第 2 の置換手段それぞれに与える中間鍵を生成する鍵生成手段を備えるとともに、

前記第 1 及び第 2 の置換手段は、前記鍵生成手段が生成した中間鍵に所定の情報が含まれているときには恒等変換として機能することを特徴とする請求項 1 又は 2 記載の暗復号装置。

【請求項 4】 前記第 1 及び又は第 3 の暗号復号化手段は、前記鍵生成手段が生成した中間鍵に所定の情報が含まれているときには、前記第 2 の暗号復号化手段と同一のアルゴリズムに従う手段となることを特徴とする請求項 3 記載の暗復号装置。

【請求項 5】 前記第 2 の暗復号化手段は、前記第 1 及び第 3 の暗号復号化

手段が暗号化処理を行うときには復号処理を実行し、前記第 1 及び第 3 の暗号復号化手段が復号処理を行うときには暗号化処理を実行することを特徴とする請求項 3 又は 4 記載の暗復号装置。

【請求項 6】 前記鍵生成手段は、前記第 1 及び第 3 の暗号復号化手段に同一の中間鍵を与えることを特徴とする請求項 5 記載の暗復号装置。

【請求項 7】 前記鍵生成手段は、前記第 1 及び第 2 の暗号復号化手段、又は、前記第 2 及び第 3 の暗号復号化手段が同一アルゴリズムとなりかつ同一暗復号鍵を使用する結果となる中間鍵を与えることを特徴とする請求項 5 記載の暗復号装置。

【請求項 8】 平文を暗号文に暗号化し、及び又は、暗号文を平文に復号する暗復号装置を制御するプログラムであって、

暗号処理又は復号処理を行わせる第 1 の暗復号化手段と、

前記第 1 の暗復号化手段の出力を所定の置換表によりデータ置換させる第 1 の置換手段と、

前記第 1 の置換手段の出力に対し、暗号処理又は復号処理を行わせる第 2 の暗復号化手段と、

前記第 2 の暗復号化手段の出力を所定の置換表によりデータ置換させる第 2 の置換手段と、

前記第 2 の置換手段の出力に対し、暗号処理又は復号処理を行わせる第 3 の暗復号化手段と

を有するプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項 9】 前記第 1、第 2 及び第 3 の暗復号化手段並びに前記第 1 及び第 2 の置換手段それぞれに与える中間鍵を生成させる鍵生成手段を備えるとともに、

前記第 1 及び第 2 の置換手段を、前記鍵生成手段が生成させた中間鍵に所定の情報が含まれているときには恒等変換として機能させることを特徴とする請求項 8 記載の記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は暗復号装置及び記憶媒体、特に秘密鍵ブロック暗号により情報を暗号化若しくは復号するのに適した暗復号装置及び記憶媒体に関するものである。

【0002】

【従来の技術】

近年の計算機通信技術の発達に伴い、種々の情報がデジタル情報として通信され、また蓄積されるようになってきているが、これらの情報についての機密やプライバシーを保護するために情報を暗号化する必要性が増している。このために、従来は主にDES方式（特開昭51-108701）を用いることで、情報の暗号を図っている。

【0003】

しかしながら、DES方式（以下、単にDESともいう）は1970年代に設計された暗号アルゴリズムであり現代の技術進歩に対して安全であるとは言えなくなっている。DESに対する解読攻撃方法としては、56ビットからなる鍵の総当り探索や総当り探索より効率のよい差分攻撃（E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Journal of CRYPTOLOGY, Vol. 4, Number 1, 1991）、線形攻撃（松井充, DES暗号の線形解読法（I）, 暗号と情報セキュリティシンポジウム, 1993）等が知られている。

【0004】

このような状況から既に広く普及しているDES方式を大幅に変更することなく、解読攻撃に対する防御力を強化する試みとして、トリプルDESが知られている。

【0005】

トリプルDESは暗号化を行うのにDESを3回適用する方式であり、2つの鍵を使用して、鍵1による暗号化、鍵2による復号、鍵1による暗号化、という手順により暗号化を行うものである。トリプルDESではDESの鍵を2つ用いるので個々の鍵は56ビットでありながら、実質的な鍵の長さは112ビットで

あると考えることができる。

【0006】

しかし、トリプルDESはDESを3回行うため、DESと較べて処理時間が多くかかってしまうという問題点がある。

【0007】

一方、DESを強くしようとする異なる試みとして、DES-SS方式（特開平10-116029）が知られている。

【0008】

DES-SS方式（以下、単にDES-SSともいう）では、DES内部で使われている非線型関数であるF関数の他に新たにG関数を用いることで、DESの安全性を高めている。また、DES-SSの処理ではDESと比較するとG関数の処理が増加しているだけなので、トリプルDESと較べて効率がよいという特徴を持つ。

【0009】

さらに、トリプルDESとは異なり56ビットの鍵を複数用いるのではなく、1個の鍵自体の長さが112ビットであるため、総当り攻撃に対してより安全であるという特徴も持っている。

【0010】

DESの56ビットの鍵は8ビットのパリティビットを含めて64ビットで表される。DES-SSでは、鍵の上位64ビットと下位64ビットが同じ値である場合には、DESと同じ機能を果たす暗号化関数として動作するという他の暗号方式にない特徴がある。これによりDES-SSを有する暗復号装置では、DES互換モードを設けることが可能になる。

【0011】

このDES互換モードの原理は、鍵の上位と下位が等しい場合には、G関数の入力と出力が一致する関数、すなわち恒等変換であることに基づいている。DES-SSのもつDES互換モードを利用することにより、1つの暗復号装置で2つの暗号化を行うことができ、装置規模を小さくできるという利点がある。

【0012】

【発明が解決しようとする課題】

上記したように、DES、トリプルDES、DES-SSにはそれぞれ長所と短所がある。ここで、情報暗号化の要請及び高強度の必要性がますます高くなっていること、及び、DESは広く普及していること、等の事情を考え合わせれば、DES及びその応用暗号化技術との互換性を確保しつつ強度の高い暗号化も可能な技術を提供することが重要になってきている。

【0013】

しかし、この技術の実現にあたっては、暗号の効率性という点も考慮に入れなければならない。

【0014】

例えばDES-SSを用いれば、DESより安全でトリプルDESより効率のよい暗号化を行うことができる。ここでDES-SSを用いてトリプルDESと互換性のある暗号を構成しようとする場合を考える。DES-SSを3段重ねることでトリプルDESと互換性のある暗号を実現することは可能ではあるが、トリプルDES以上に効率が悪くなるという問題がある。

【0015】

一方、DES、トリプルDES及びDES-SSの何れもラウンド関数を利用し、同じ構造の処理を繰り返し行う積暗号と呼ばれる形式を用いている。このような形式の暗号は、上記した差分攻撃や線形攻撃に弱いという特徴を持っている。

【0016】

本発明は、このような実情を考慮してなされたもので、DES、トリプルDES、DES-SSのすべてと互換な単一の暗号アルゴリズムを構成するが、単にDES-SSを3段重ねるより効率がよく、かつ差分攻撃や線形攻撃にも強いアルゴリズムとなる暗復号装置及び記憶媒体を提供することを目的とする。

【0017】

【課題を解決するための手段】

上記課題を解決するために、請求項1に対応する発明は、平文を暗号文に暗号化し、及び又は、暗号文を平文に復号する暗復号装置であって、暗号処理又は復

号処理を行う第1の暗復号化手段と、第1の暗復号化手段の出力を所定の置換表によりデータ置換する第1の置換手段と、第1の置換手段の出力に対し、暗号処理又は復号処理を行う第2の暗復号化手段と、第2の暗復号化手段の出力を所定の置換表によりデータ置換する第2の置換手段と、第2の置換手段の出力に対し、暗号処理又は復号処理を行う第3の暗復号化手段とを備えた暗復号装置である。

【0018】

本発明はこのような手段を設けたので、各暗復号化手段の内容及び各置換手段の使用有無を調整することで、DES、トリプルDES、DES-SSのすべてと互換な単一の暗号アルゴリズムを構成するが、単にDES-SSを3段重ねるより効率がよいものとすることができる。また、置換手段によりデータ置換を行えば、データの連続性に擾乱が与えられるので、差分攻撃や線形攻撃にも強いアルゴリズムとすることができる。

【0019】

次に、請求項2に対応する発明は、請求項1に対応する発明において、第1の暗復号化手段と第3の暗復号化手段、並びに、第1の置換手段と第2の置換手段は、それぞれ同一のアルゴリズムに従う手段となる暗復号装置である。

【0020】

本発明はこのような手段を設けたので、より簡単な構成で請求項1に係る発明と同様な効果を得ることができる。

【0021】

次に、請求項3に対応する発明は、請求項1又は2に対応する発明において、第1、第2及び第3の暗復号化手段並びに第1及び第2の置換手段それぞれに与える中間鍵を生成する鍵生成手段を備えたとともに、第1及び第2の置換手段は、鍵生成手段が生成した中間鍵に所定の情報が含まれているときには恒等変換として機能する暗復号装置である。

【0022】

本発明はこのような手段を設けたので、第1及び第2の置換手段に与える中間鍵の内容を制御することで、DES、トリプルDES等の互換モードとそれ以外

の強化暗号モードを容易に切り換えることができる。

【0023】

次に、請求項4に対応する発明は、請求項3に対応する発明において、第1及び又は第3の暗号復号化手段は、鍵生成手段が生成した中間鍵に所定の情報が含まれているときには、第2の暗号復号化手段と同一のアルゴリズムに従う手段となる暗復号装置である。

【0024】

本発明はこのような手段を設けたので、第1～第3の暗復号化手段に与える中間鍵の内容を制御することで、DES、トリプルDES等の互換モードにおける各モード切替を容易に行うことができる。

【0025】

次に、請求項5に対応する発明は、請求項3又は4に対応する発明において、第2の暗復号化手段は、第1及び第3の暗号復号化手段が暗号化処理を行うときには復号処理を実行し、第1及び第3の暗号復号化手段が復号処理を行うときには暗号化処理を実行する暗復号装置である。

【0026】

本発明はこのような手段を設けたので、容易にトリプルDESやDES、DES-SS間の切り替えを行うことができる。

【0027】

次に、請求項6に対応する発明は、請求項5に対応する発明において、鍵生成手段は、第1及び第3の暗号復号化手段に同一の中間鍵を与える暗復号装置である。

【0028】

本発明はこのような手段を設けたので、容易にトリプルDESを実現することができる。

【0029】

次に、請求項7に対応する発明は、請求項5に対応する発明において、鍵生成手段は、第1及び第2の暗号復号化手段、又は、第2及び第3の暗号復号化手段が同一アルゴリズムとなりかつ同一暗復号鍵を使用する結果となる中間鍵を与え

る暗復号装置である。

【0030】

本発明はこのような手段を設けたので、容易にDESやDES-Sを實現することができる。

【0031】

次に、請求項8に対応する発明は、請求項1に対応する発明をコンピュータに實現させるプログラムを記録した記録媒体である。

【0032】

この記録媒体から読み出されたプログラムにより制御されるコンピュータは、請求項1の暗復号装置として機能する。

【0033】

次に、請求項9に対応する発明は、請求項6に対応する発明をコンピュータに實現させるプログラムを記録した記録媒体である。

【0034】

この記録媒体から読み出されたプログラムにより制御されるコンピュータは、請求項3の暗復号装置として機能する。

【0035】

【発明の実施の形態】

以下、本発明の実施の形態について説明する。

(発明の第1の実施の形態)

図1は本発明の第1の実施形態に係る暗復号装置の一例を示す構成図である。

【0036】

この暗復号装置10は、第1、第2、第3暗復号化部11、13、15、第1、第2置換処理部12、14並びに鍵スケジュール部16を備える他、各機能部11～16を制御する制御部(図示せず)を備えて、暗号化装置、復号装置あるいは暗号化・復号装置として構成される。

【0037】

ここで、平文21を第1暗復号化部11に入力し、第1置換処理部12、第2暗復号化部13、第2置換処理部14、第3暗復号化部15と処理を進めて暗号

文 2 2 を出力する場合には暗号装置として機能し、暗号文 2 2 を第 3 暗復号化部 1 5 に入力し、上記と逆方向に処理を進める場合には復号装置として機能する。この何れの装置として、機能させるかは制御部の処理によって決まることになる。

【0038】

また、暗復号装置 1 0 は、ハードウェア的には CPU やメモリ等の計算機要素から構成されるものである。各機能部 1 1 ~ 1 6 はこの計算機要素が所定のプログラムに制御されて実現される。すなわち機能部 1 1 ~ 1 6 はハードウェア資源とソフトウェア資源の結合たる機能実現手段である。また、上記計算機要素及びプログラムは、パーソナルコンピュータやワークステーション等の計算機に提供されるものを使用するか、専用のチップを作成することにより、本暗復号装置 1 0 用に確保される。

【0039】

次に、上記各機能部 1 1 ~ 1 6 の構成について説明する。

【0040】

まず、鍵スケジュール部 1 6 は、外部から入力された鍵情報 K をもとに中間鍵に展開し、機能部 1 1 ~ 1 5 からなるデータ攪拌部に供給する。

【0041】

機能部 1 1 ~ 1 5 からなるデータ攪拌部は、64 ビット入力の平文 2 1 又は暗号文 2 2 を、鍵スケジュール部 1 6 からの鍵により攪拌して暗号化しあるいは復号し、対応する暗号文 2 2 若しくは平文 2 1 として出力する。

【0042】

ここで、第 1 暗復号部 1 1 は、DES-SS のデータ攪拌部と同様な構成を備え、平文 2 1 を入力され、鍵スケジュール部 1 6 から入力された中間鍵の制御下で暗号化処理としての攪拌処理を行い、出力を第 1 置換処理部 1 2 に入力する。逆に、第 1 置換処理部 1 2 からの入力を鍵スケジュール部 1 6 からの中間鍵で復号し、平文 2 1 として出力する。なお、復号処理については、ここで説明したように暗号化処理の逆の処理を行うだけなので、以下の機能部 1 2 ~ 1 5 の説明においては暗号化を行う場合についてのみ説明し、特に断らない限り復号について

は省略する。

【0043】

また、この第1暗復号部11は、DES-Sの構成を有することから、鍵スケジュール部16からの中間鍵の内容が一定の場合には単なるDESとして機能する。なお、DES-Sについては第2の実施形態で詳しく説明する。

【0044】

第1置換処理部12は、第1暗復号処理部11から入力されたデータについて、中間鍵及び置換表を用いたデータの置換処理を行い、その出力を第2暗復号化部13に入力する。また、中間鍵が一定の場合にはこの第1置換処理部12を未使用状態にできるようになっている。未使用状態の場合は入力データをそのまま出力する。ここで、置換表は、乱数によって生成する方法若しくは代数的に生成する方法（式を用いる方法）によって作成される。何れの場合も差分確率及び線形確率の低い、すなわち差分攻撃や線形攻撃に強い置換表を作成する。

【0045】

図2は置換処理部等に用いられる差分確率及び線形確率の低い置換表の一例を示す図である。

【0046】

このような表は、差分確率及び線形確率の良好（低く）にできる代数式（例えば有限体GF(2⁸)上で原始多項式($x^8 + x^4 + x^3 + x^2 + 1$)を用いて x^{-1} を計算する；“^”は冪乗演算）を用いるか、差分確率及び線形確率が良くなるまで乱数計算を繰り返して作成する。

【0047】

なお、本実施形態において差分確率及び線形確率が良好であるためには、それぞれの確率が理想値の2倍以下であることが望ましい。ここで8ビットの場合であれば、差分確率の理想値は $4/256$ であり、線形確率の理想値は $16/256$ である。

【0048】

次に第2暗復号化部13は、DESのデータ攪拌部と同様な構成を備え、第1置換処理部12からの出力に対し、鍵スケジュール部16からの中間鍵の制御下

で攪拌処理を行い、その出力を第2置換処理部14に入力する。なお、ここにおける攪拌処理は暗号文22を生成するための復号処理である。逆に平文21に復号するためには暗号処理がなされる。

【0049】

第2置換処理部14は、第1置換処理部13と同様な構成を備え、中間鍵および置換表を用いたデータの置換処理を行い、出力を第3暗復号化部15に入力する。また、中間鍵が一定の場合には第2置換処理部14を未使用状態、すなわち入力と出力が一致するようになっている。

【0050】

第3暗復号部15は、DES-SSのデータ攪拌部と同様な構成を備え、鍵スケジュール部16から入力された中間鍵の制御下で暗号化処理としての攪拌処理を行い、暗号文22を出力する。また、第3暗復号部15もDES-SSの構成を有するので、鍵スケジュール部16からの中間鍵の内容が一定の場合には単なるDESとして機能する。

【0051】

次に、以上のように構成された本実施形態における暗復号装置の動作について説明する。

【0052】

この暗復号装置においては、鍵スケジュール部16からの中間鍵により、第1、第3暗復号処理部11、15を、“DES”、“DES-SS”の何れか、また第1、第2置換処理部12、14を、“使用”、“未使用”の何れかの状態に選択できるようになっている。これにより各機能部11～15の状態組み合わせを適宜に変更可能である。

【0053】

図3は各機能部の状態組み合わせの例を示す図である。

【0054】

同図において、まず、第1、第3暗復号化部11、15をDESモードにし、第1、第2置換処理部12、14を未使用の状態にするとともに、第1、第2暗復号化部11、13に使用する鍵を同一にすると、暗復号装置全体はDESによ

る暗復号装置となる。

【0055】

これは、第2暗復号化部13が平文21の暗号化に際して復号処理を行うため、第1暗復号処理部11で暗号化されたデータが第2暗復号化部13によって元の平文21に戻ってしまうためである。

【0056】

次に、第1、第2、第3暗復号化部11、13、15をDESモードにし、第1、第2置換処理部12、14を未使用状態とすると、トリプルDESと同一の状態になる。トリプルDESは、平文を第1の鍵で暗号化し、その出力を第2の鍵で復号し、さらにその出力を第1の鍵で暗号化する方式である。ここでは、第1暗復号化部11が上記最初の暗号化を担当し、第2暗復号化部13が次の復号を担当し、第3暗復号化部15が最後の暗号化を担当する。

【0057】

次に、第1暗復号化部11をDESモードにし、第1、第2置換処理部12、14を未使用状態とするとともに、第1、第2暗復号化部11、13に同一の鍵を使用するとDES-SSモードと同一の状態になる。上記の場合と同様に、第1、第2暗復号化部11、13の処理は互いにうち消し合って、平文21が第3暗復号化部15に入力される状態になるためである。

【0058】

以上が本実施形態の暗復号装置10の有するDES、トリプルDES、DES-SS互換モードである。

【0059】

次に、第1、第2置換処理部12、14を使用する場合には、上記互換モードよりも強化された暗号化を行うモードとなる。以下に説明する各場合は、第1、第2置換処理部12、14を使用するものである。

【0060】

例えば第1、第2、第3暗号化部11、13、15すべてをオリジナルのモード(DES-SS、DES、DES-SS)で使用した場合(図3:パターン1)、トリプルDESとDES-SSを組み合わせ、さらに各処理間に置換表によ

る攪拌を加えたものとなる。

【0061】

この場合、DES方式に類するラウンド関数の繰り返しによるデータ攪拌がDES-SSの長い鍵で十分に行われるとともに、各処理間で差分確率及び線形確率の低い置換表による攪拌が加えられるので、データの連続性に擾乱がおり、線形攻撃や差分攻撃といった攻撃に対する防御力が強くなる。

【0062】

また、第1、第3暗復号化部11、15をDESとし（図3：パターン2）、線形攻撃等からの防御力を保持しつつ、パターン1に比べて暗号化時間の短縮化を図るようにすることも可能である。

【0063】

さらに、第1、第3暗復号化部11、15の一方をDESとし、他方をDES-SSとしてパターン1とパターン2の中間的な暗号とすることも可能である。

【0064】

また、上記各パターンの場合に、各暗復号化部11、13、15に与える鍵の組み合わせを変更して更に種々の暗号形式とすることができる。例えば暗復号化部11、13、15すべてに異なる鍵を与える、暗復号化部11、13に同一の鍵を与える、暗復号化部11、15に同一の鍵を与える、暗復号化部13、15に同一の鍵を与える、暗復号化部11、13、15すべてに同一の鍵を与える、等のパターンが考えられる。

【0065】

これらは、暗復号化装置10の処理能力や、互換モード及び強化暗号モードにおける各パターンの普及度等を考慮して適宜選択される。

【0066】

上述したように、本発明の実施の形態に係る暗復号装置は、第1、第2、第3暗復号化部11、13、15を設け、各処理部の動作モード及び与える鍵を適宜変更できるようにしたので、DES、トリプルDES、DES-SSのすべてと互換な単一の暗号アルゴリズムを構成するが、DES-SSを3段重ねるより効率のよい暗号アルゴリズムの装置として構成することができる。したがって、こ

のような暗号アルゴリズムの装置では独立して3つの暗号装置を持つよりも、装置規模を小さくすることができる。

【0067】

また、本実施形態の暗復号装置10は、置換処理部12, 14によって、データの連続性に擾乱を起こすことができるので、線形攻撃や差分攻撃等の同一構成の繰返しに着目した攻撃をより困難にすることができ、安全性を向上させることができる。

【0068】

また、本実施形態の装置では、単一のアルゴリズムで種々の暗号方式を提供できるので、各暗号の普及度やハードウェアの処理能力の変化に応じて使用する暗号方式を選択することができ、長期間に渡って使用することができる。

(発明の第2の実施の形態)

本実施形態では、第1の実施形態における各機能部11~16の構成をより具体化させた場合について説明する。したがって、本実施形態は第1の実施形態と同様に構成される他、各機能部11~16における更なる形態例が示されるものである。

【0069】

本実施形態の暗復号装置10は、図1に示す第1の実施形態の暗復号装置と同様に構成されている。以下、各機能部11~16の構成例を説明する。なお、本実施形態の各図面においては、第1実施形態の図1と同一部分には同一符号を付して詳細説明を省略する。

[鍵スケジュール部16の構成動作]

まず、鍵スケジュール部16について説明する。

【0070】

図4は鍵スケジュール部の全体構成を示す図である。

【0071】

同図に示すように、鍵スケジュール部16には、256ビットの鍵情報Kを5つに分割し各レジスタ32, 33, 34, 35, 36に格納する分割部31と、レジスタ32~35から56ビットの鍵情報を読み出しこれを拡大転置して64ビ

ットにする拡大転置部37とが設けられている。さらに、拡大転置結果若しくはレジスタ36の内容から中間鍵K1, K2, K3並びにKK1及びKK2をそれぞれ生成するDES-SS鍵スケジュール部38, 39、DES鍵スケジュール部40及び置換用鍵スケジュール部41が設けられ、鍵スケジュール部16が構成されている。

【0072】

ここで256ビットの鍵情報は、分割部31において56ビットからなる4つのブロックB1, B2, B3, B4と、32ビットの1つのブロックB5に分割され、それぞれレジスタ32～36に記憶される。この場合の分割の仕方は、256ビットを先頭から順次56ビットずつ切り出してそれぞれB1～B4とし、さらに最後の残り32ビットをB5とするものである。

【0073】

また、ブロックB1からブロックB4までの4つのブロックはそれぞれ拡大転置部37に入力され、それぞれ拡大転置表によって64ビットに拡大される。

【0074】

図5は拡大転置表の一例を示す図である。

【0075】

同図の表は先頭から出力ビットに対応しており、また各出力ビットにおける数字は入力第nビット目であることをあらわす。ただし、表中の0はその出力ビットとして0が出力されることを表す。

【0076】

次に、ブロックB1を拡大した64ビットの鍵とブロックB2を拡大した64ビットの鍵を連結した128ビットの鍵は、第1暗復号部11への中間鍵K1を出力するDES-SS鍵スケジュール部38に入力される。

【0077】

また、ブロックB1を拡大した64ビットの鍵とブロックB3を拡大した64ビットの鍵を連結した128ビットの鍵は、第3暗復号部15への中間鍵K3を出力するDES-SS鍵スケジュール部39に入力される。

【0078】

また、ブロックB4を拡大した64ビットの鍵は、第2暗復号部15への中間鍵K2を出力するDES鍵スケジュール部40に入力される。さらに、32ビットのブロックB5は拡大転置されることなく置換用鍵スケジュール部41に入力される。

【0079】

上記各鍵スケジュール部38～41のうち、DES鍵スケジュール部40は一般的なDESにおける拡大鍵生成手段と同様な構成を有するのみであるので、詳細説明は省略し、以下、DES-SS鍵スケジュール部38、39及び置換用鍵スケジュール部41について説明する。

【0080】

図6はDES-SS鍵スケジュール部の構成例を示すブロック図である。

【0081】

DES-SS鍵スケジュール部38、39は、Aスケジュール部45、Bスケジュール部46及びFG拡大鍵生成部47から構成される。なお、FG拡大鍵生成部47は各ラウンド（1段～16段）に対応して設けられるとともに、Aスケジュール部45及びBスケジュール部46内も16段の構成となっており、同図にはそれぞれ第1段のみが示されている。なお、符号以外の同図における数値はビット数を現している。

【0082】

拡大転置部37から入力される128ビットの鍵のうち、各ブロックB1、B2若しくはB3に対応する部分がそれぞれAスケジュール部45、Bスケジュール部46に入力されるようになっている。

【0083】

Aスケジュール部45及びBスケジュール部46は、入力される鍵が異なり、また拡大鍵を生成するためのデータの出力の仕方が異なる点を除けば、一般的なDESにおける拡大鍵生成手段と同様な構成となっているので詳細説明は省略する。

【0084】

ここで、DES-SS用とDES用の中間鍵における相違点は、DES-SS

ではDESの攪拌手段に使用されるF関数拡大鍵に加え、G関数拡大鍵が必要な点である。

【0085】

図6におけるAスケジュール部45及びBスケジュール部46では、ビット選択部48A、48Bが中間鍵K1/K2を生成するための情報を入力する。

【0086】

ここでまず、Aスケジュール部45のビット選択部48Aは、F関数拡大鍵FK1を出力するとともに、5ビットの鍵A1を出力する。この5ビットの鍵A1は例えばビット選択部48Aに入力されてなる56ビットの鍵の左から9, 18, 22, 25, 35番目の5ビットが用いられる。この5ビット選択方法は他の方法でも良い。

【0087】

一方、Bスケジュール部4のビット選択部48Bは、G関数拡大鍵の元になる48ビットの鍵GB1を出力するとともに、鍵A1と同様な5ビットの鍵B1を出力する。Aスケジュール部45及びBスケジュール部46が一般的なDESの拡大鍵生成手段と異なるのは、ビット選択部48A、48B（以下の、2～16段も同様）の処理がこのように修正されている点のみである。

【0088】

FG拡大鍵生成部47は、ビット選択部48Aが出力した鍵をそのままF関数拡大鍵FK1として出力する。また、48ビットの鍵GB1とF関数拡大鍵FK1の排他的論理和49をとってG関数拡大鍵GK1の一部（G1, G2, G3）として出力する。さらにFG拡大鍵生成部47は、鍵A1と鍵B1との間で排他的論理和50を取り、さらにその出力と0X10（0Xは16進を表す）との間で排他的論理和51をとってG関数拡大鍵GK1の一部（G4）として出力する。

【0089】

こうして、DES-SS鍵スケジュール部38, 39によって、F関数拡大鍵FK1と、鍵G1, G2, G3, G4からなるG関数拡大鍵GK1とを含む中間鍵K1, K3が得られる。

【0090】

DES-SS鍵スケジュール部38が出力した中間鍵K1は第1暗復号化部11に入力され、DES-SS鍵スケジュール部39が出力した中間鍵K3は第3暗復号化部15に入力されることとなる。なお、詳細説明は省略したが、DES鍵スケジュール部40が出力した中間鍵K2は第2暗復号化部13に入力され、第2暗復号化部13によって、DESによる暗復号が実行される。

【0091】

次に、置換用鍵スケジュール部41について説明する。

【0092】

図7は置換用鍵スケジュール部の構成例を示すブロック図である。

【0093】

この置換用鍵スケジュール部41は、レジスタ36のブロックB5を32ビットの鍵として入力し、第1置換処理部12に入力される中間鍵KK1と、第2置換処理部14に入力される中間鍵KK2を出力するものである。

【0094】

まず、レジスタ54内の32ビットの鍵C0'は、そのまま第1置換処理部12用の中間鍵KD1（32ビット）として出力されるとともに、論理和部55及び左シフト部56に入力される。なお、レジスタ54はレジスタ36と同一であってもよい。

【0095】

論理和部55では、32ビットの鍵C0'における各ビットの論理和が計算結果として出力され、第1置換処理部12用の中間鍵KS1（1ビット）となる。

【0096】

この中間鍵KD1と中間鍵KS1とから中間鍵KK1が構成され、第1置換処理部12に入力される。

【0097】

次に、左シフト部56に入力されたデータは同シフト部56により4ビットほど左シフトされた後、鍵C1としてレジスタ57に格納される。

【0098】

この鍵C1'は、第2置換処理部14に入力される32ビットの中間鍵KD2となり、また、論理和部58において32ビットC1'の論理和の計算結果が、第2置換処理部14に入力される1ビットの中間鍵KS2となる。

【0099】

この中間鍵KD2と中間鍵KS2とから中間鍵KK2が構成され、第2置換処理部14に入力される。

【0100】

以上が鍵スケジュール部16の構成及び動作であり、次に、置換処理部12, 14について説明する。

[置換処理部12, 14の構成動作]

図8は置換処理部の構成例を示すブロック図である。

【0101】

同図に示すように置換処理部12, 14は、初期転置部61と、排他的論理和62～66と、置換部67～74と、逆転置部75とから構成されている。置換部67～74には、図2に示すような置換表が保持されており、入力を置換表により変換して出力する。

【0102】

ここで、まず、暗復号化部からの64ビットの入力は、初期転置（初期転置IP）部61においてビット転置が行われ、その結果が8ビットずつの8つのブロックに分割される。

【0103】

初期転置61の出力のうち8ビットブロック4つからなる32ビットはそのまま置換部67～70に入力される。残りの8ビットブロック4つからなる32ビットは排他的論理和62～66において中間鍵KD（中間鍵KD1/KD2）との排他的論理和が行われ、その結果が置換部71～74に入力される。

【0104】

置換部67～74には、8ビットの入力データと1ビットの鍵KS（中間鍵KS1/KS2）とが入力される。ここで、鍵ビットが1の場合には、置換表を用いた入力に対応する出力データが出力され、鍵ビットが0の場合には、入力と同

一の出力データが出力される。すなわち鍵 K_S が 0 ビットの場合には置換処理部 12, 14 は未使用状態となる。

【0105】

各置換部 67~74 からの出力は逆転置 (逆転置 IP^{-1}) 75 に入力され、ここでビット転置が行われたのち、64 ビットデータとして出力される。

[第 1, 第 3 暗復号化部 11, 15 の構成動作]

次に、DES-SS のデータ攪拌手段として構成される第 1, 第 3 暗復号化部 11, 15 について説明する。

【0106】

図 9 は DES-SS として構成された暗復号化部の構成例を示すブロック図である。

【0107】

DES-SS として構成された第 1, 第 3 暗復号化部 11, 15 は、鍵 GK 及び FK からなる中間鍵 K_1 又は K_3 に依存して入力 (64 ビット) を攪拌し、対応する暗号文を出力する。この暗復号化部 11, 15 は、初期転置部 (初期転置 IP) 80 と、第 1 段から第 16 段までのデータ攪拌部 81~96 と、最終転置部 (最終転置 IP^{-1}) 97 とから構成されている。各データ攪拌部 81~96 は、暗号化関数としての F 関数 81f~96f 及び排他的論理和 81a~96a を備えて DES のデータ攪拌手段と同様に構成される他、鍵 GK を用いてデータを攪拌する暗号化関数としての G 関数 81g~96g をも備えている。

【0108】

ここで、 F 関数 81f~96f は、通常の DES と同様な攪拌処理を行うものであり、中間鍵 K_1 , K_3 のうちの F 関数拡大鍵 FK と G 関数 81g~96g の出力とを受け、所定の攪拌処理を行ってその結果を排他的論理和 81a~96a に入力する。

【0109】

排他的論理和 81a~96a は、32 ビットの L_n ($L_0 \sim L_{15}$) と F 関数 81f~96f の出力との間の排他的論理和を次段の入力の右側 32 ビット R_{n+1} として出力する。

【0110】

また、G関数 81g～96gは、後述する攪拌処理を行うものであり、中間鍵 K1、K3のうちのG関数拡大鍵GKとRn（R0～R15）を受け、所定の攪拌処理を行って次段の入力の左側32ビットLn+1及びF関数 81f～96fへ出力する。

【0111】

各段のデータ攪拌部 81～96では同様な処理が実行される。まず第1段の動作について説明する。

【0112】

暗復号化部 11、15において、入力（64ビット）は初期転置部 80にて転置された後、2つに等分割されて左側32ビットL0と右側32ビットR0として生成される。

【0113】

第1段データ攪拌部 81において、R0は暗号化G関数 81gに入力され、そのG関数出力が暗号化F関数 81fに入力されるとともに、第2段データ攪拌部 82に左側32ビットL1として出力される。一方、L0は排他的論理和部 81aに入力され、F関数 81fとの間で排他的論理和が取られた後、第2段データ攪拌部 82に右側32ビットR1として出力される。

【0114】

以上の攪拌処理が第1段で行われたのち、以下、第16段まで第1段と同様の攪拌処理が行われる。第16段の出力は最終転置部 97によって転置が行われた後、64ビットの出力となる。

【0115】

次にG関数 81g～96gにおける処理について説明する。

【0116】

図10はG関数の構成例を示すブロック図である。

【0117】

このG関数 81g～96gは、入力データに対し、G関数拡大鍵GKに含まれる4つの鍵G1、G2、G3、G4を用いた攪拌を行ってデータ出力するもので

ある。このために、G関数 81g~96gは、排他的論理和部 103, 104, 108、論理積部 101, 106、左シフト部 105を備えている。

【0118】

なお、同図に示す $L0'$, $L1'$, $L2'$, $L3'$, $R0'$, $R1'$, $L2'$, $R3'$ は、これらのデータがレジスタに格納され、あるいは次の機能手段に引き渡されることを示す。

【0119】

このG関数においては、まず入力(32ビット)は、2つに等分割されて左側32ビット $L0'$ と右側32ビット $R0'$ が生成される。

【0120】

$R0'$ は論理積部 101 及び排他的論理和部 104 に入力され、 $L0'$ は排他的論理和部 103 に入力される。

【0121】

論理積部 101 において $R0'$ と拡大鍵 G1 の論理積が行われ、排他的論理和部 103 に出力される。排他的論理和 103 においては $L0'$ と論理積部 101 の出力との排他的論理和が行われ、その結果 $L1'$ が左シフト 105 に入力される。

【0122】

一方、排他的論理和 104 においては $R0'$ と拡大鍵 G2 との排他的論理和が行われ、その結果 $R1'$ が左シフト部 105 に入力される。

【0123】

左シフト部 105 においては、拡大鍵 G4 のビット数に従った左シフトが行われ、そのシフト結果の出力は2つに等分割して左側32ビットが $R2'$ に、右側32ビットが $L2'$ となる。

【0124】

$R2'$ は論理積部 106 に入力され、 $L2'$ は排他的論理和部 108 に入力される。論理積部 106 においては $R2'$ と拡大鍵 G3 の論理積が行われ、排他的論理和部 108 に出力される。

【0125】

さらに、排他的論理和部 108 において、 $L2'$ と論理積部 106 の出力との排他的論理和が行われ、G 関数の出力の左側 32 ビットとなる。一方、G 関数の出力の右側 32 ビットは $R2'$ が用いられる。

【0126】

この G 関数においては、入力を分割しその分割入力を再び接続してシフトしつつ、その間に攪拌処理を挿入して出力データの攪拌度合いを高いものになっている。

【第 2 暗復号化部 13 の構成動作】

第 2 暗号化部 13 は、一般的な DES のデータ攪拌手段と同様に構成されているので、ここでは詳細な説明は省略する。なお、DES のデータ攪拌手段については（岡本栄司著、「暗号理論入門」，共立出版，1993）等に記載されている。また、例えば図 9 に示す DES-SS の構成から G 関数 81g~96g を取り除き G 関数拡大鍵 GK を不要としたものは、DES のデータ攪拌手段の一例となっている。

【鍵情報 K に対応した暗復号装置 10 の動作】

本実施形態の暗復号装置 10 の各機能部 11~16 が上記したように構成され動作するときに、鍵スケジュール部 16 に与える鍵情報 K の内容により、暗復号装置 10 がいかなる内容の暗号若しくは復号装置となるかについて説明する。

【0127】

ここで、鍵情報 K は、図 4 に示すように、ブロック B1~B5 に分割されるものであり、各ブロック B1~B5 の内容がどのようなになっているかにより本装置 10 における処理が決まることになる。

【0128】

まず、ブロック B5 の部分に少なくともビットが立っており、その論理和 55, 58 が 0 にならない場合には、鍵 KS が 0 とならずひいては図 8 に示す置換処理部 12, 14 における置換部 67~74 において置換処理が実行される。この場合には、暗復号装置 10 は、図 3 における強化暗号モードとして動作する。この結果、従来の DES、DES-SS 又はトリプル DES とは異なり、置換表による暗号連続性が擾乱された暗号となって、より強化された暗号化が実現される。

【0129】

特に、ブロック B 1 からブロック B 5 の鍵情報として独立したものを与えれば、より安全性の高い 256 ビット鍵の暗号化アルゴリズムとして使用される。

【0130】

一方、置換用鍵スケジュール部 4 1 に入力される 32 ビットの鍵ブロック B 5 の入力ビットがすべて 0 である場合には論理和 55, 58 の出力である鍵 K S が 0 になるため、置換処理部 12 及び 14 における置換表が使用されない。したがって、この場合の中間鍵 K K 1, K K 2 によっては、置換処理部 12 及び 14 において、入力と同一のデータが出力され恒等変換が行われることになる。

【0131】

置換処理部 12 及び 14 にて恒等変換が行われる場合には、暗復号装置 10 は図 3 における互換モードとして動作することになる。以下、この場合について、更に具体的に説明する。

【0132】

まず、図 4 において、ブロック B 1 と同一の内容をブロック B 2 及び B 3 に入力することにより、DES-S 鍵スケジュール部 38 及び 39 は、第 1, 第 3 暗復号化部 11, 15 が DES 暗号化モードとなる暗号化処理を行う中間鍵を生成する。第 1, 第 3 暗復号化部 11, 15 が DES モードになるためには、図 9 における G 関数入出力が恒等変換となればよい。この恒等変換は、図 10 に示す G 関数処理において、拡大鍵 G 1 ~ G 4 が所定の入力になれば実現される。

【0133】

このとき、暗号化装置全体としては、ブロック B 1 に入力された鍵ビットによる第 1 暗復号化部 11 の DES 暗号化と、ブロック B 4 に入力された鍵ビットによる第 2 暗復号化部 13 の DES 復号の処理となり、56 ビットからなる 2 つの鍵を用いたトリプル DES と同一の処理内容となる。

【0134】

この場合に、さらにブロック B 1 とブロック B 4 に同一の内容を用い、ブロック B 2 と B 3 のいずれか一方をブロック B 1 と同一の内容に設定することにより

、DES-SSとの互換モードとして動作する。これは、ブロックB1と同一内容を入力する側の暗復号化部11又は15がDESモードで動作して、第2暗復号化部13の処理とキャンセルするため、結果としてDES-SSモードの部分のみが残るからである。

【0135】

このとき、例えばブロックB3をブロックB1と同一の内容とすると、暗号化装置10全体としては、ブロックB1とB2をそれぞれ拡大転置した出力を結合した128ビットの鍵を入力とするDES-SSと同一の処理内容となる。

【0136】

上述したように、本発明の実施の形態に係る暗復号装置は、256ビットの鍵情報Kを5つのブロックに分割し、各ブロック情報を用いて実質的な中間鍵情報のみならず、第1、第2置換処理部12、14の使用有無、及び、第1、第2、第3暗復号化部11、13、15の動作モード指定ができる情報を生成し、これによって装置全体の動作モードを制御するようにしたので、第1の実施形態と同様な装置を実現させ、その作用効果を得ることができる。

【0137】

すなわち本実施形態では、鍵情報Kの内容を修正するだけで動作モードの変更を容易に行うことができ、DES、トリプルDES、DES-SSのすべてと互換な単一の暗号アルゴリズムを構成するとともに、データの連続性に擾乱を起せる線形攻撃や差分攻撃等に強い暗号をも実現させることができる。

(発明の第3の実施の形態)

本実施形態は、第2の実施形態における第1、第3暗復号化部11、15のG関数に改良を加えた場合について説明する。

【0138】

図11は本発明の第3の実施形態に係る暗復号装置におけるG関数の構成例を示すブロック図であり、図1～図10と同一部分には同一符号を付して説明を省略する。

【0139】

この暗復号装置10は、図11に示すように、第1、第3暗復号化部11、1

5のG関数81g～96gにおいて、論理積101～排他的論理和103間に置換部102，論理積106～排他的論理和108間に置換部107が挿入される他、第2の実施形態と同様に構成されている。したがって、本実施形態にて説明するG関数81g～96gは厳密にはDES-SSのG関数とは異なるものであり、DES-SS用のG関数が修正されたものである。

【0140】

置換部102，107は、差分の一様性および非線形性の高い特性を有する、例えば図2に示すような置換表を保持しており、入力を置換表により変換して出力する。

【0141】

このように構成された本実施形態の暗復号装置10は第2の実施形態と同様に動作する他、新たな付加された置換部102，107部分については以下のように動作する。

【0142】

まず、置換部102においては、論理積101の出力が入力されるようになっている。この論理積出力は置換表にて置換され、その結果が排他的論理和103に出力される。

【0143】

また、置換部107においては、論理積106の出力が入力されるようになっている。この論理積出力は、置換部102の場合と同様に置換表にて置換され、その結果が排他的論理和108に出力される。

【0144】

本実施形態のG関数81g～96gでは、その中に差分確率及び線形確率が低い置換表による置換102，107が挿入されているために、データの連続性に擾乱が起こされ、線形攻撃や差分攻撃に強い暗号化が実現されている。

【0145】

この置換部102，107に用いる置換表として、本実施形態では図2に示す表を用いると説明したが、この変形例として図2の置換表をアフィン変換して入力0に対する出力が0である置換表を用いることも考えられる。このとき、特定

の鍵入力の場合には置換部 102, 107 の出力が 0 となり、排他的論理和部 103 及び 108 における鍵情報の挿入が行われなくなる。したがって、このような置換表を用いた場合には、G 関数は入力と出力が一致する恒等変換の関数として機能することも可能になる。

【0146】

上記置換部 102, 107 を用いることにより、論理積部 101 及び 106 における鍵との論理積の結果、論理積の出力ビットの 0 ビットと 1 ビットの出現率に不均一性が現れても、置換部 102, 107 の処理により、この不均一性を是正し、鍵に含まれる 1 ビットの数に着目した攻撃に対して安全になる。

【0147】

例えば拡大鍵 G1 に出現する 1 ビットの数がある場合には、排他的論理和部 103 においてさされる鍵、すなわち排他的論理和が行われる実質ビット数は高々 1 ビットである。しかし、置換部 102 による置換の結果、さされる鍵のビット数は変化し、鍵に含まれる 1 ビットの数に着目した攻撃に対して安全になる。

【0148】

上述したように、本発明の実施の形態に係る暗復号装置は、G 関数に置換部 102, 107 を挿入したので、データの連続性に擾乱が起こされ、線形攻撃や差分攻撃に強い暗号化を実現することができる。

【0149】

なお、実施形態に説明した装置は、記憶媒体に格納したプログラムをコンピュータに読み込ませることで実現させることができる。

【0150】

ここで本発明における記憶媒体としては、磁気ディスク、フロッピーディスク、ハードディスク、光ディスク（CD-ROM、CD-R、DVD 等）、光磁気ディスク（MO 等）、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であってもよい。

【0151】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基

づきコンピュータ上で稼働しているOS（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のMW（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行してもよい。

【0152】

さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶又は一時記憶した記憶媒体も含まれる。

【0153】

また、記憶媒体は1つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何らの構成であってもよい。

【0154】

なお、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であってもよい。

【0155】

また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【0156】

【発明の効果】

以上詳記したように本発明によれば、DES、トリプルDES、DES-SSのすべてと互換な単一の暗号アルゴリズムを構成するが、単にDES-SSを3段重ねるより効率がよく、かつ差分攻撃や線形攻撃にも強いアルゴリズムとなる暗復号装置及び記憶媒体を提供することができる。

【図面の簡単な説明】

【図1】

本発明の第1の実施形態に係る暗復号装置の一例を示す構成図。

【図 2】

置換処理部等に用いられる差分確率及び線形確率の低い置換表の一例を示す図

【図 3】

各機能部の状態組み合わせの例を示す図。

【図 4】

鍵スケジュール部の全体構成を示す図。

【図 5】

拡大転置表の一例を示す図。

【図 6】

DES-SS 鍵スケジュール部の構成例を示すブロック図。

【図 7】

置換用鍵スケジュール部の構成例を示すブロック図。

【図 8】

置換処理部の構成例を示すブロック図。

【図 9】

DES-SS として構成された暗復号化部の構成例を示すブロック図。

【図 10】

G 関数の構成例を示すブロック図。

【図 11】

本発明の第 3 の実施形態に係る暗復号装置における G 関数の構成例を示すブロック図。

【符号の説明】

10…暗復号装置

11…第 1 暗復号化部

12…第 1 置換処理部

13…第 2 暗復号化部

14…第 2 置換処理部

15…第 3 暗復号化部

16…鍵スケジュール部
21…平文
22…暗号文
31…分割部
37…拡大転置部
38, 39…DES-SS鍵スケジュール部
40…DES鍵スケジュール部
41…置換用鍵スケジュール部
45…Aスケジュール部
46…Bスケジュール部
47…FG拡大鍵生成部
48A, 48B…ビット選択部
49, 50…排他的論理和
55, 58…論理和部
56…左シフト部
61…初期転置部
62～66…排他的論理和
67～74…置換部
75…逆転置部
80…初期転置部
81～96…データ攪拌部
81a～96a…排他的論理和
81f～96f…F関数
81g～96g…G関数
97…最終転置部
101, 106…論理積部
102, 107…置換部
103, 104, 108…排他的論理和部
105…左シフト部

B 1 ～ B 4 … ブロック

F K … F 関数拡大鍵

G 1 ～ G 4 … 拡大鍵

G K … G 関数拡大鍵

K 1 … 第 1 暗復号化部への中間鍵

K 2 … 第 2 暗復号化部への中間鍵

K 3 … 第 3 暗復号化部への中間鍵

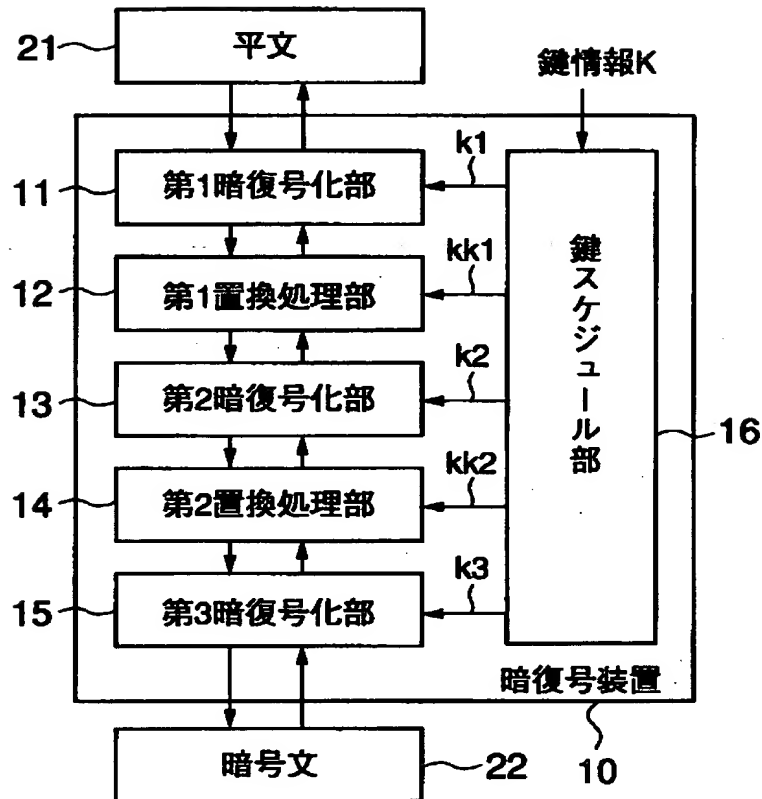
K K 1 … 第 1 置換処理部への中間鍵

K K 2 … 第 2 置換処理部への中間鍵

【書類名】

図面

【図 1】



【図 2】

置換表

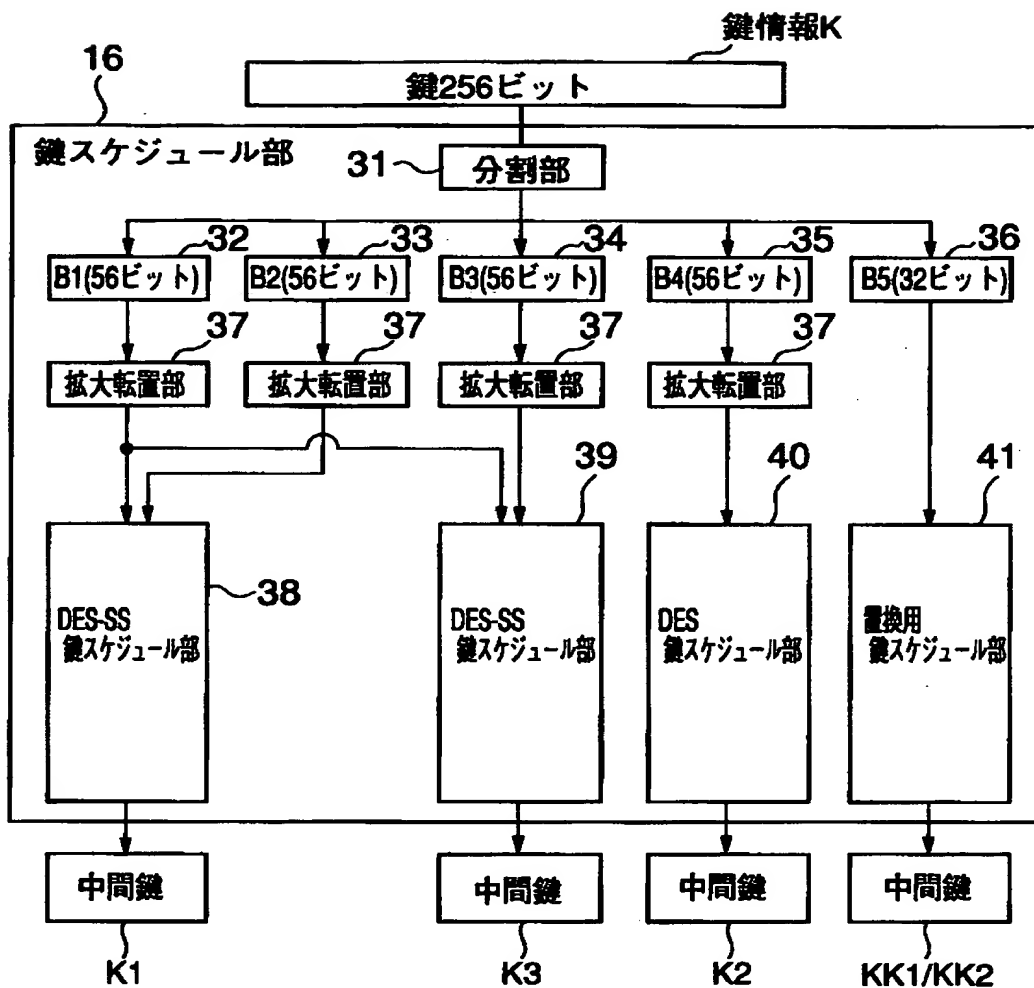
0	1142	244	71	167	122	186	173	157	221	152	61	170	93	150	
216	114	192	88	224	62	76	102	144	222	85	128	160	131	75	42
108	237	57	81	96	86	44	138	112	208	31	74	38	139	51	110
72	137	111	46	164	195	64	94	80	34	207	169	171	12	21	225
54	95	248	213	146	78	166	4	48	136	43	30	22	103	69	147
56	35	104	140	129	26	37	97	19	193	203	99	151	14	55	65
36	87	202	91	185	196	23	77	82	141	239	179	32	236	47	50
40	209	17	217	233	251	218	121	219	119	6	187	132	205	254	252
27	84	161	29	124	204	228	176	73	49	39	45	83	105	2	245
24	223	68	79	155	188	15	92	11	220	189	148	172	9	199	162
28	130	159	198	52	194	70	5	206	59	13	60	156	8	190	183
135	229	238	107	235	242	191	175	197	100	7	123	149	154	174	182
18	89	165	53	101	184	163	158	210	247	98	90	133	125	168	58
41	113	200	246	249	67	215	214	16	115	118	120	153	10	25	145
20	63	230	240	134	177	226	241	250	116	243	180	109	33	178	106
227	231	181	234	3	143	211	201	66	212	232	117	127	255	126	253

【図3】

	互換モード				強化暗号モード		
第1暗復号化部	DES	DES	DES	DES	DES-SS	DES	...
第1置換処理部	未使用	未使用	未使用	未使用	使用	使用	
第2暗復号化部	DES	DES	DES	DES	DES	DES	
第2置換処理部	未使用	未使用	未使用	未使用	使用	使用	
第3暗復号化部	DES	DES	DES	DES-SS	DES-SS	DES	
得られる暗号	DES ^{*1}	トリプルDES ^{*2}	DES-SS ^{*3}	DES-SS ^{*3}	パターン1	パターン2	...

- *1：第1、第2暗復号化部で同一の鍵を使用する
- *2：第1、第3暗復号化部で同一の鍵、第2暗復号化部で異なる鍵を使用する
- *3：第1、第2暗復号化部で同一の鍵を使用する

【図 4】

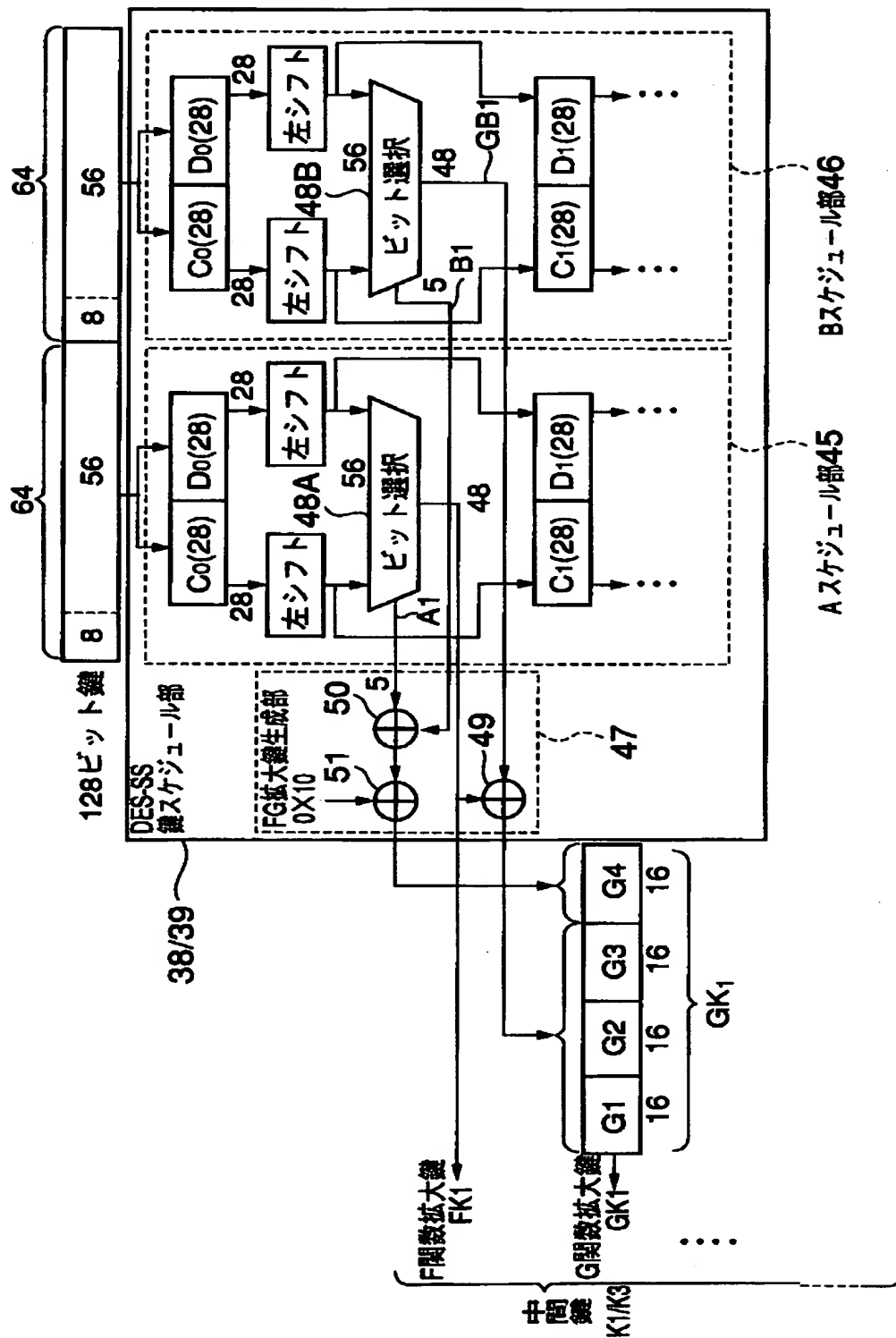


【図 5】

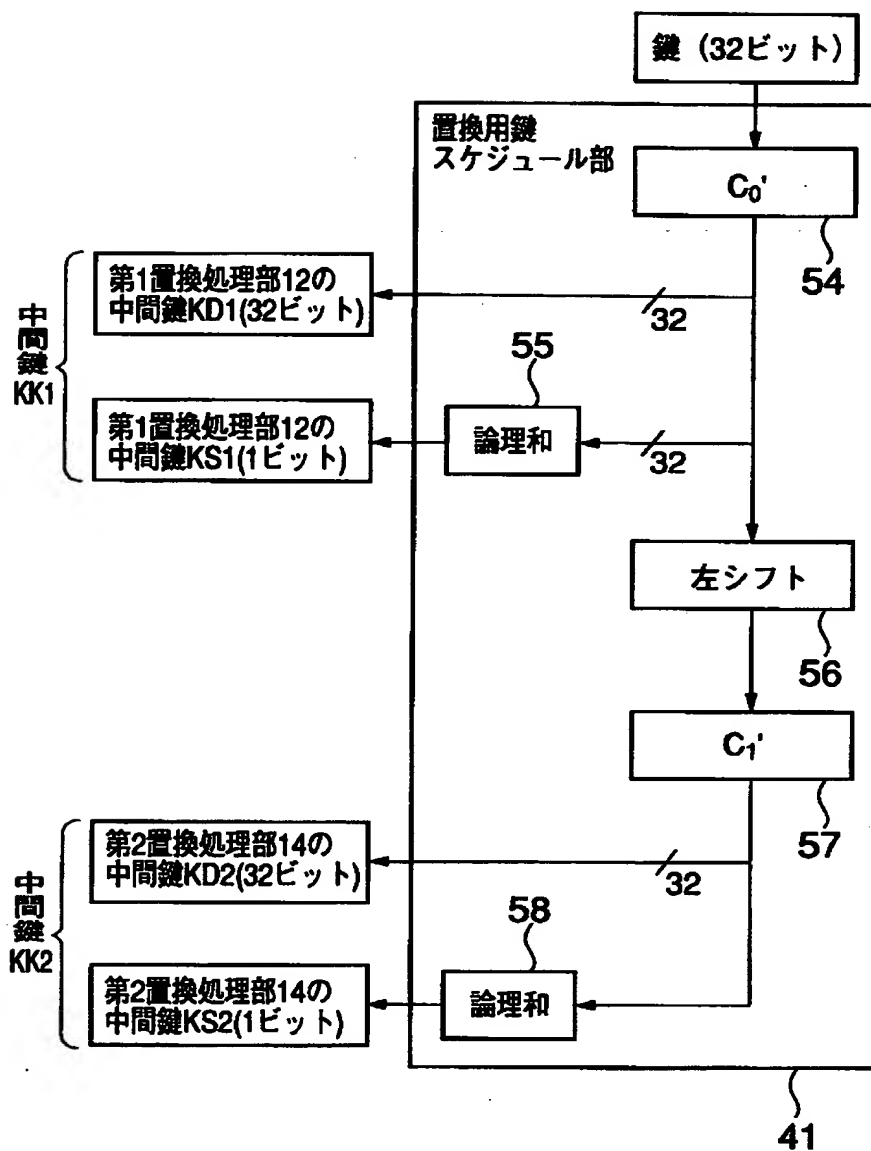
拡大転置表

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	0	17	18	19	0	20	21	0	22	23	24	25	26	27
28	30	0	31	32	0	33	34	35	36	0	37	38	39	40
42	43	44	45	46	0	47	48	49	50	51	52	53	54	55
56														

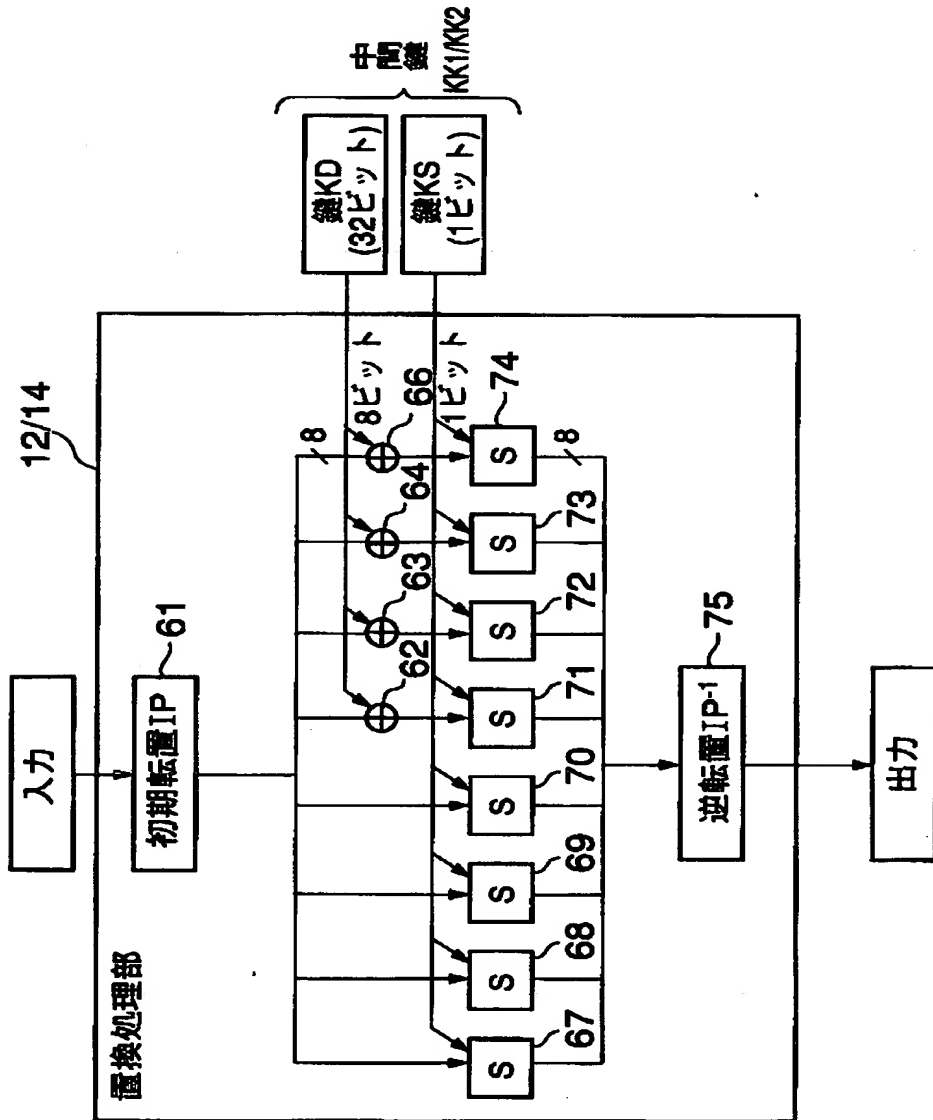
【図 6】



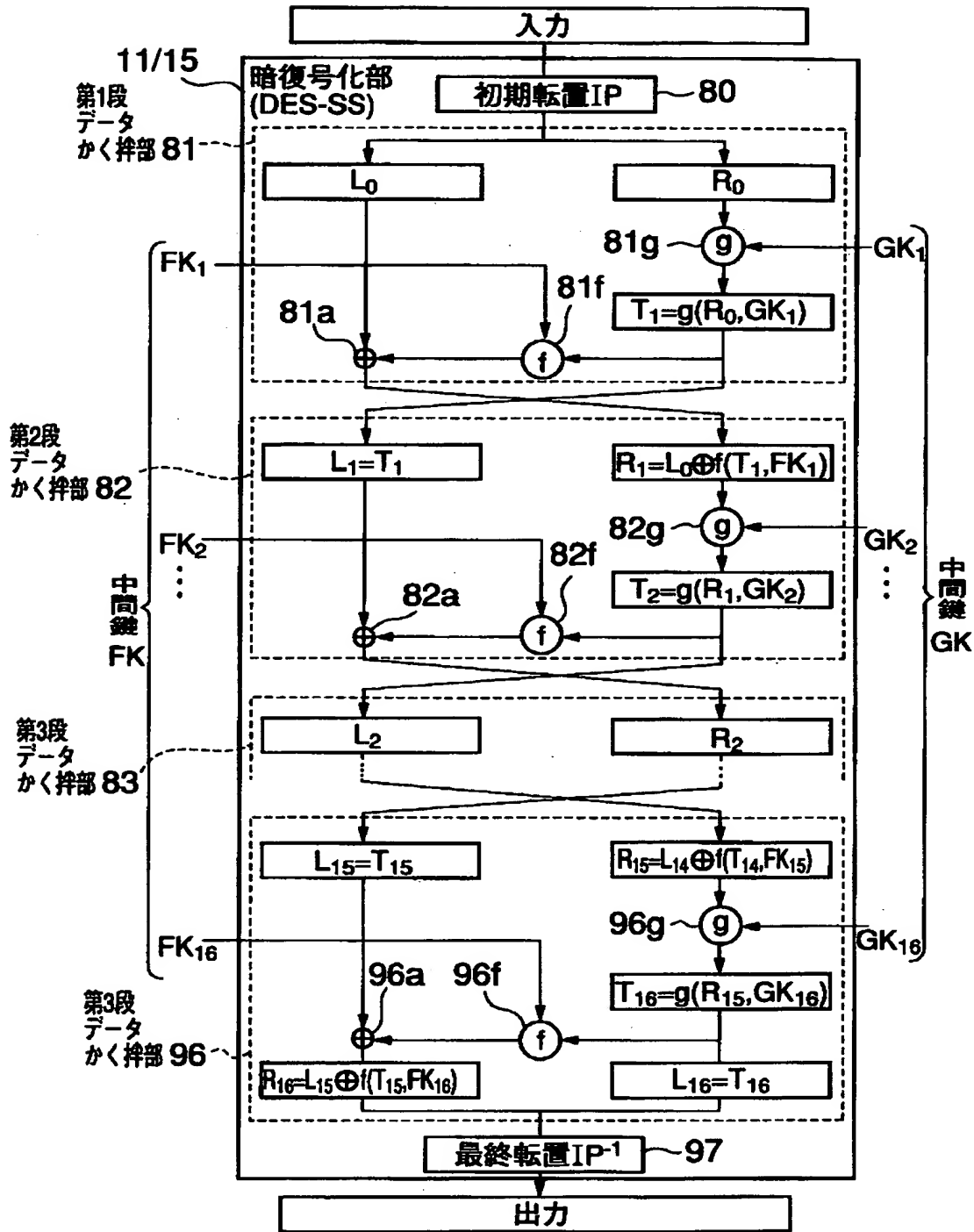
【図 7】



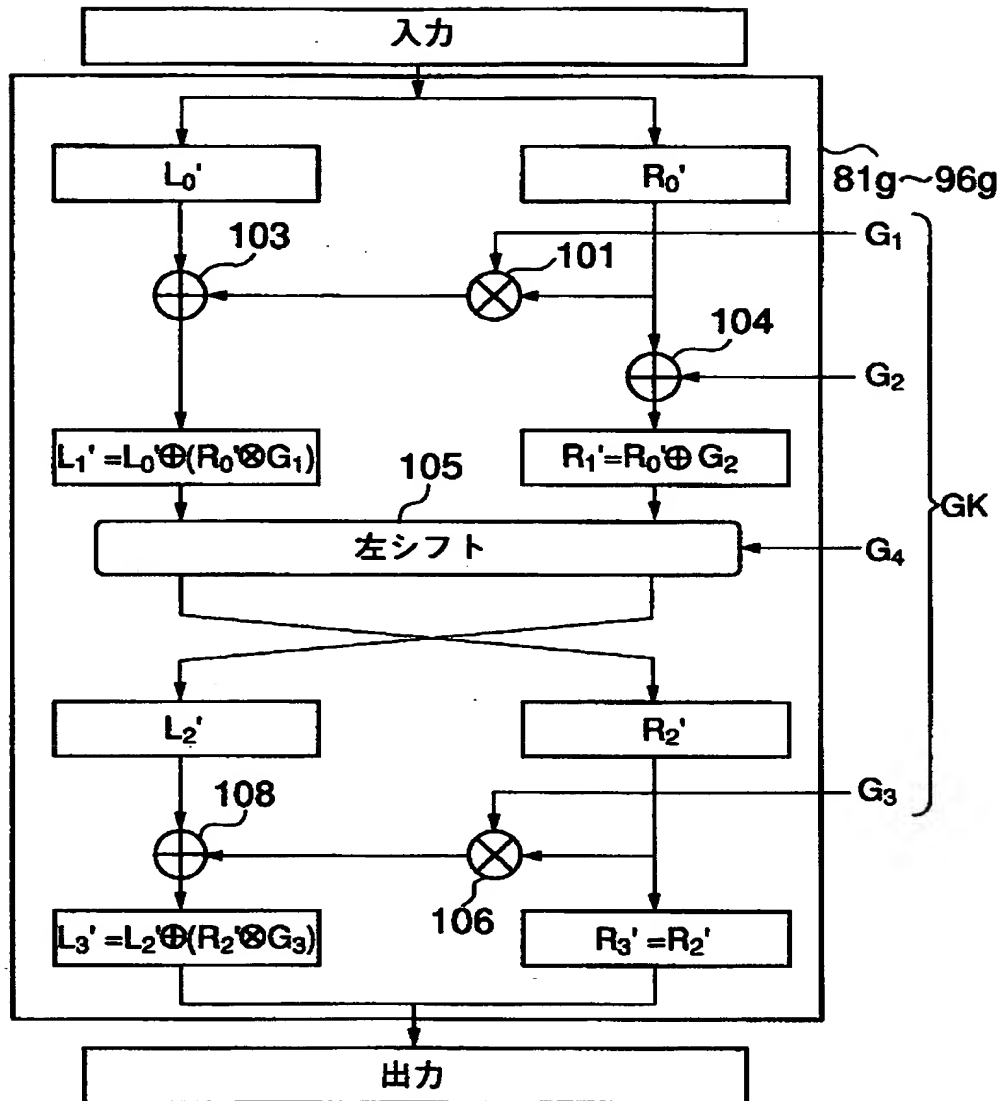
【図8】



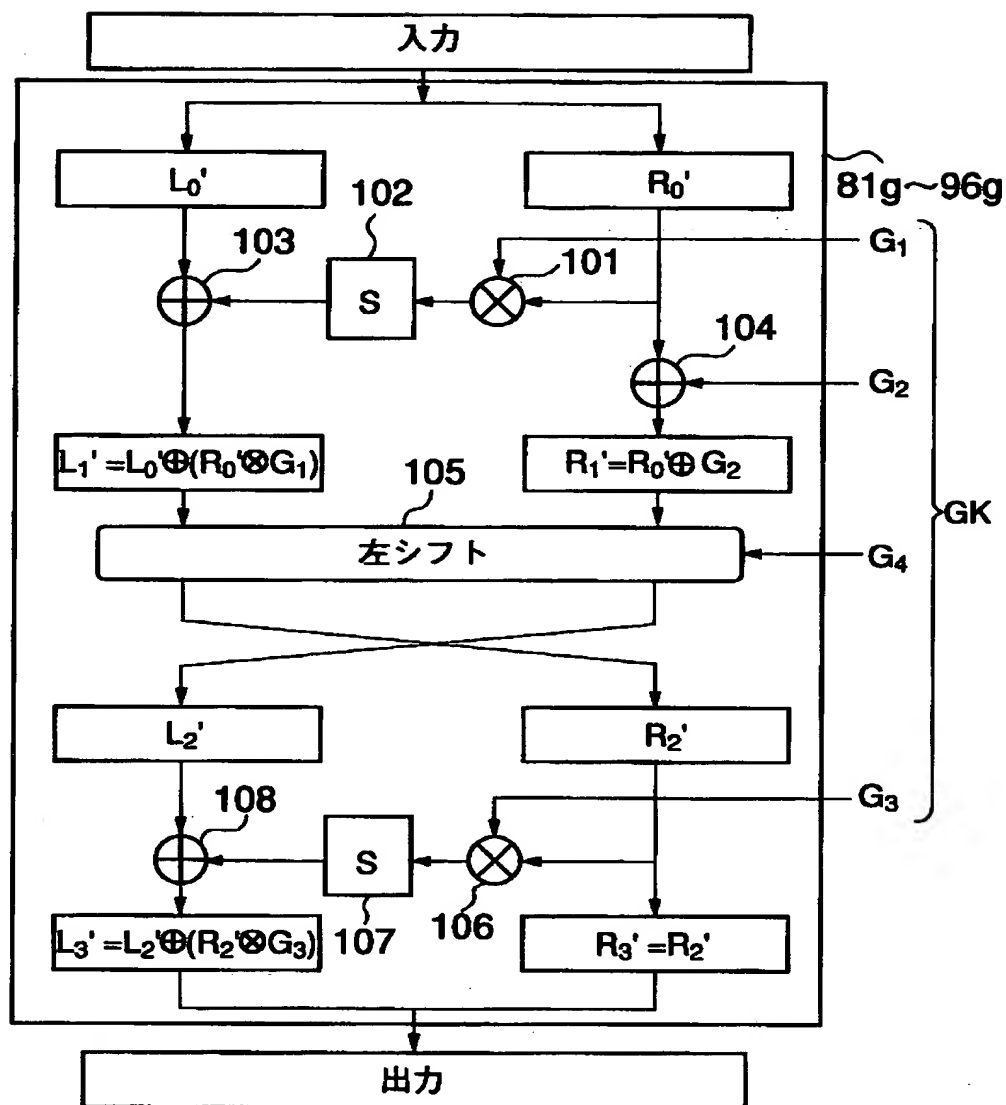
【図 9】



【図 10】



【図 11】



【書類名】 要約書

【要約】

【課題】 本発明は、DES、トリプルDES、DES-SSのすべてと互換な単一の暗号アルゴリズムを構成するが、単にDES-SSを3段重ねるより効率がよく、かつ差分攻撃や線形攻撃にも強いアルゴリズムとなる。

【解決手段】 平文21を暗号文22に暗号化し、及び又は、暗号文を平文に復号する暗復号装置10であって、暗号処理又は復号処理を行う第1の暗復号化手段11と、第1の暗復号化手段の出力を所定の置換表によりデータ置換する第1の置換手段12と、第1の置換手段の出力に対し、暗号処理又は復号処理を行う第2の暗復号化手段13と、第2の暗復号化手段の出力を所定の置換表によりデータ置換する第2の置換手段14と、第2の置換手段の出力に対し、暗号処理又は復号処理を行う第3の暗復号化手段15とを備えた暗復号装置

【選択図】 図1

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】
【識別番号】 000003078
【住所又は居所】 神奈川県川崎市幸区堀川町7番地
【氏名又は名称】 株式会社東芝
【代理人】 申請人
【識別番号】 100058479
【住所又は居所】 東京都千代田区霞が関3丁目7番2号 鈴榮内外國
特許法律事務所内
【氏名又は名称】 鈴江 武彦
【選任した代理人】
【識別番号】 100084618
【住所又は居所】 東京都千代田区霞が関3丁目7番2号 鈴榮内外國
特許法律事務所内
【氏名又は名称】 村松 貞男
【選任した代理人】
【識別番号】 100068814
【住所又は居所】 東京都千代田区霞が関3丁目7番2号 鈴榮内外國
特許法律事務所内
【氏名又は名称】 坪井 淳
【選任した代理人】
【識別番号】 100092196
【住所又は居所】 東京都千代田区霞が関3丁目7番2号 鈴榮内外國
特許法律事務所内
【氏名又は名称】 橋本 良郎
【選任した代理人】
【識別番号】 100091351
【住所又は居所】 東京都千代田区霞が関3丁目7番2号 鈴榮内外國
特許法律事務所内
【氏名又は名称】 河野 哲
【選任した代理人】
【識別番号】 100088683
【住所又は居所】 東京都千代田区霞が関3丁目7番2号 鈴榮内外國
特許法律事務所内
【氏名又は名称】 中村 誠
【選任した代理人】

特平 10-337108

【識別番号】	100070437
【住所又は居所】	東京都千代田区霞が関3丁目7番2号 鈴榮内外國 特許法律事務所内
【氏名又は名称】	河井 将次

出 願 人 履 歷 情 報

識別番号 [000003078]

1. 変更年月日	1990年 8月22日
[変更理由]	新規登録
住 所	神奈川県川崎市幸区堀川町72番地
氏 名	株式会社東芝